REMARKS

Claims 1-25 were previously pending in this application. By this amendment, Applicant is canceling claims 2-3, 6, 8-9, 11-12, 17-18, and 22-25 without prejudice or disclaimer. Claims 1, 4, 7, 10, 13-14, 16, 19, and 21 have been amended. As a result, claims 1, 4-5, 7, 10, 13-16, and 19-21 are pending for examination with claims 1, 16, 19, and 21 being independent claims. No new matter has been added. This preliminary amendment is responsive to the Final Office Action (hereinafter the "Office Action") mailed January 23, 2008.

Rejection Under 35 U.S.C. §101

Claims 21-25 were rejected under 35 U.S.C. §101 as it is alleged in the Office Action that the claimed invention is directed to non-statutory subject matter. Although Applicant does not concede that claims 21-25 are drawn to non-statutory subject matter under 35 U.S.C. §101, Applicant has amended claim 21 to be more clear, and also notes that claims 22-25 were canceled. In particular, claim 21, as amended now recites a "distributed computer system" which is an article of manufacture which is statutory subject matter under 35 U.S.C. §101. Further, it is not understood from the Office Action under what authority the alleged "software" can be rejected – claim 21 was originally drawn to an apparatus, which is a machine, and claim 21 is now drawn to a distributed computer system which is also a machine. Applicant is not aware any precedent of a 35 U.S.C. §101 rejection of an "apparatus" claim that could relate to software. The Examiner is encouraged to cite the proper basis for rejecting claims under 35 U.S.C. §101, or withdraw such rejections. Therefore, Applicant respectfully requests that the rejection of claim 21 be withdrawn.

Rejections Under 35 U.S.C. §102

The Office Action rejected claims 1-5 and 21 under 35 U.S.C. §102(b) as being anticipated by Del Monte (U.S. Publication Number 2004/0024823, hereinafter "Del Monte"). In response, Applicant has amended the independent claims and submits the following remarks.

Del Monte is directed to a method for authenticating incoming email (Abstract). The method and system comprise a server that intercepts incoming emails, authenticates them on behalf of the intended recipient, and either makes them available to the recipient if they are desirable, or discards them if they are not (Abstract). The system of Del Monte provides a

system for preventing unsolicited emails, commonly known as junk or spam, from reaching end users (Abstract). In particular, in paragraph [0037], Del Monte describes an authentication process that identifies the "from" address in the header (the "sender") and uses a rule set to determine if this sender is allowed to send email to the recipient (Please see paragraphs [0037]-[0042]).

By contrast, independent claim 1, as amended, recites, in a distributed computer system, a method for locating a discrepancy in mapping information that maps an identifier to a particular resource in a domain naming system database, the method comprising acts of compiling a list of nameservers to be queried comprising acts of sending a namespace mapping resolution query to a plurality of network nodes; waiting for one or more responses from the plurality of network nodes; and determining whether a network node in the plurality of network nodes is a nameserver based on a format of one or more responses received from the network node; if the network node is a nameserver, adding the network node to the list of nameservers to be queried; determining a first mapping in a domain naming system, the act of determining the first mapping comprising an act of obtaining an authoritative mapping from an authoritative source; determining a second mapping in the domain naming system, the act of determining a second mapping comprising acts of querying a nameserver of the list of nameservers to be queried and receiving a response from the nameserver, the response containing the second mapping, wherein the first mapping is a first namespace mapping that maps a first name to a first resource and the second mapping is a second namespace mapping that maps a second name to a second resource; comparing the first mapping to the second mapping and identifying at least one discrepancy between the first and second mapping; and generating and sending an alert message to a user, the alert message indicating the at least one discrepancy between the first and second mapping.

Del Monte does not disclose that which is recited in claim 1, as amended. In particular, Del Monte does not disclose "compiling a list of nameservers to be queried comprising acts of sending a namespace mapping resolution query to a plurality of network nodes; waiting for one or more responses from the plurality of network nodes; determining whether a network node in the plurality of network nodes is a nameserver based on a format of one or more responses received from the network node; and if the network node is a nameserver, adding the network node to the list of nameservers to be queried," as recited in claim 1 as amended. Del Monte is not concerned with nameservers and maintaining lists of nameservers as recited in claim 1; Del

Monte is concerned with preventing spam email by checking a received email header to determine is a particular sender is among a list of approved senders. Therefore, Del Monte does not disclose that which is recited in claim 1, as amended. Claims 4-5, 7, 10, and 13-15 depend from claim 1 and are allowable for at least the same reasons.

Claims 1-8, 10 and 21-24 were rejected under 35 U.S.C. §102(e) as being anticipated by Hrabik et al., (U.S. Publication Number 2002/0178383, hereinafter "Hrabik"). In response, Applicant has amended independent claims 1 and 21, and submits the following remarks.

Hrabik is directed to a system for verifying the integrity of devices on a target network (Abstract). The apparatus has security subsystems and a master security system hierarchically connected to the security subsystems via a secure link (Abstract). The target network includes various intrusion detection devices, which may be part of the security subsystem (Abstract). Each intrusion detection device generates a plurality of event messages when an attack on the network is detected (Abstract). The security subsystem collects these event messages, correlates, and analyzes them, and performs network scanning processes (Abstract). If certain events warrant additional scrutiny, they are uploaded to the master security system for review (Abstract).

Hrabik also discusses, in Paragraph [0069]:

In addition to the vulnerability and visibility scans, the master system 60 also verifies services that directly affect the target network's connectivity but are typically out of the network's control. This verification assessment ensures that company's domain name was not "hijacked." The master security system conducts a verification assessment of all information sources involved in network connectivity verifying information from a root domain name servers all the way through to a primary and a secondary web servers. The verification scan is performed for the entire IP address group of the target company. For example, when a target company has six IP addresses four of which are open and utilized and two of which are blocked and not accessible, the verification scan determines whether the blocked addresses remain unaccessible and whether the open addresses remain accessible. The assessment also includes a verification that when users are trying to access the network's website by typing "www.company.com," they get to the proper website and their e-mail goes to the proper server. The master system also verifies information at the Whois database of the registration provider to ensure that contact and

authorization information has not been changed. To protect target's website, the master system may also check whether the text, graphics and other information contained on the website was not altered by intruders. The master system may also test functionality of target's e-commerce and other on-line applications to assure that the entire web system is operational and any problems may be addressed immediately. The master system also tests and verifies external (Internet) routing information, DNS info, netbios information, access control, etc. (Paragraph [0069] of Hrabik.)

Hrabik does not disclose that which is recited in claim 1, as amended. In particular, Hrabik does not disclose "compiling a list of nameservers to be queried comprising acts of sending a namespace mapping resolution query to a plurality of network nodes; waiting for one or more responses from the plurality of network nodes; determining whether a network node in the plurality of network nodes is a nameserver based on a format of one or more responses received from the network node; and if the network node is a nameserver, adding the network node to the list of nameservers to be queried," as recited in claim 1 as amended. Hrabik is not concerned with nameservers and maintaining lists of nameservers as recited in claim 1. More particularly, Hrabik is concerned with making sure a computer can get to a particular network's website, e-mail of a user goes to the proper server, and that information at a Whois database of the registration provider to ensure that contact and authorization information has not been changed (Please see paragraph [0069]). Hrabik mentions that DNS information may be tested and verified, but provides no details of how this could possibly be accomplished. Further, the Office Action admits that Hrabik does disclose an act of compiling a list of nameservers to be queried (Paragraph 7 of the Office Action). Therefore, Hrabik does not disclose that which is recited in claim 1, as amended. Claims 4-5, 7, 10, and 13-15 depend from claim 1 and are allowable for at least the same reasons.

Independent claim 21, as amended, recites a distributed computer system for locating discrepancies in domain name databases, the distributed computer system comprising:a detector adapted to determine a first mapping and a second mapping, wherein the detector is further adapted to compare the first mapping to the second mapping and to identify at least one discrepancy between the first mapping and second mapping, wherein the apparatus is configured to obtain an authoritative mapping from an authoritative source and store the authoritative mapping in the database; a discoverer adapted to discover at least one nameserver among a

plurality of network nodes; a database configured to store the first mapping and the second mapping and a list of a plurality of discovered nameservers, including the at least one nameserver, wherein the apparatus is configured to query the at least one nameserver, and store the second mapping contained within a response received from the nameserver, wherein the discoverer is adapted to send a namespace mapping resolution query to a plurality of network nodes, wait for one or more responses from the plurality of network nodes, determine whether a network node in the plurality of network nodes is a nameserver based on a format of one or more responses received from the network node, and if the network node is a nameserver, storing the network node to the list of nameservers to be queried; and a component adapted to generate an alert message and send the alert message to a user, the alert message indicating the at least one discrepancy between the first mapping and the second mapping.

Hrabik does not disclose that which is recited in claim 21. In particular, Hrabik does not disclose "a discoverer adapted to discover at least one nameserver among a plurality of network nodes; a database configured to store the first mapping and the second mapping and a list of a plurality of discovered nameservers, including the at least one nameserver, wherein the apparatus is configured to query the at least one nameserver, and store the second mapping contained within a response received from the nameserver, wherein the discoverer is adapted to send a namespace mapping resolution query to a plurality of network nodes, wait for one or more responses from the plurality of network nodes, determine whether a network node in the plurality of network nodes is a nameserver based on a format of one or more responses received from the network node, and if the network node is a nameserver, storing the network node to the list of nameservers to be queried; and a component adapted to generate an alert message and send the alert message to a user, the alert message indicating the at least one discrepancy between the first mapping and the second mapping". Hrabik mentions that DNS information may be tested and verified, but provides no details of how this could possibly be accomplished. Further, the Office Action admits that Hrabik does disclose an act of compiling a list of nameservers to be queried (Paragraph 7 of the Office Action). Therefore, Hrabik does not disclose that which is recited in claim 21, as amended.

Claims 16-20 were rejected under 35 U.S.C. 102(b) as allegedly being anticipated by Albitz and Liu (DNS and BIND, hereinafter "Liu"). In response, Applicant has amended independent claims 16 and 19 and submits the following remarks.

Liu is directed to the conventional DNS system. Liu is referenced in the Background section of the instant Application (located on Pages 1-2 of the instant Application), and describes a conventional configuration and function of nameservers typically used in the Internet and enterprises for resolving names to IP addresses.

Independent claim 16, as amended, recites a method for discovering nameservers in a distributed computer system, comprising acts of sending a namespace mapping resolution query to a plurality of network nodes from a montoring computer system that monitors namespace mapping violations; waiting for one or more responses from at least one of the network nodes; determining whether a network node in the plurality of network nodes is a nameserver; and storing, in a storage device in the monitoring computer system, an indication that the network node is a nameserver in response to the act of determining, the indication of the network node being stored in a list of nameservers to be queried by the monitoring computer system to determine namespace mapping violations; determining a first mapping in a domain naming system, the act of determining the first mapping comprising an act of obtaining an authoritative mapping from an authoritative source; determining a second mapping in the domain naming system, the act of determining a second mapping comprising acts of querying a nameserver of the list of nameservers to be queried and receiving a response from the nameserver, the response containing the second mapping, wherein the first mapping is a first namespace mapping that maps a first name to a first resource and the second mapping is a second namespace mapping that maps a second name to a second resource; comparing the first mapping to the second mapping and identifying at least one discrepancy between the first and second mapping; and generating and sending an alert message to a user, the alert message indicating the at least one discrepancy between the first and second mapping.

Liu does not disclose that which is recited in claim 16, as amended. In particular, Liu does not disclose "storing, in a storage device in a monitoring computer, an indication that the network node is a nameserver in response to the act of determining" as recited in claim 16, as amended. In the Office Action, the Examiner argues that claim 16 is allegedly anticipated by a zone transfer, which is used to transfer address records between nameservers. In response, Applicant has amended claim 16 to recite that the indication that the network node is a nameserver is stored in a monitoring computer. Liu does not disclose, teach or suggest discovery of nameservers and storing of indication that a network node is a nameserver in a monitoring

computer. Further, claim 16 was amended to recite "the indication of the network node being stored in a list of nameservers to be queried by the monitoring computer system to determine namespace mapping violations; determining a first mapping in a domain naming system, the act of determining the first mapping comprising an act of obtaining an authoritative mapping from an authoritative source; determining a second mapping in the domain naming system, the act of determining a second mapping comprising acts of querying a nameserver of the list of nameservers to be queried and receiving a response from the nameserver, the response containing the second mapping, wherein the first mapping is a first namespace mapping that maps a first name to a first resource and the second mapping is a second namespace mapping that maps a second name to a second resource; comparing the first mapping to the second mapping and identifying at least one discrepancy between the first and second mapping; and generating and sending an alert message to a user, the alert message indicating the at least one discrepancy between the first and second mapping." Liu does not disclose determining namespace mapping violations, and maintaining lists of nameservers to be queried by a monitoring computer system. Thus, claim 16 as amended is not anticipated by Liu, and the rejection should be withdrawn. Claims 17-18 depend from claim 16 and are allowable for at least the same reasons.

Independent claim 19, as amended, recites a method for discovering nameservers in a distributed computer system, comprising acts of listening for a request from a non-authoritative nameserver to an authoritative nameserver; when the request is detected, adding the non-authoritative nameserver to a list of nameservers; and storing the list of nameservers in a memory of a monitoring computer system, the list of nameservers to be queried by the monitoring computer system to determine namespace mapping violations; determining a first mapping in a domain naming system, the act of determining the first mapping comprising an act of obtaining an authoritative mapping from an authoritative source; determining a second mapping in the domain naming system, the act of determining a second mapping comprising acts of querying a nameserver of the list of nameservers to be queried and receiving a response from the nameserver, the response containing the second mapping, wherein the first mapping is a first namespace mapping that maps a first name to a first resource and the second mapping is a second namespace mapping that maps a second name to a second resource; comparing the first mapping to the second mapping and identifying at least one discrepancy between the first and

second mapping; and generating and sending an alert message to a user, the alert message indicating the at least one discrepancy between the first and second mapping.

Liu doe not disclose that which is recited in claim 19, as amended. In particular, Liu does not disclose "adding the non-authoritative nameserver to a list of nameservers; and storing the list in a memory of a monitoring computer system," as recited in claim 19, as amended. In the Office Action, the Examiner argues that claim 19 is allegedly anticipated by caching of nameserver responses. In response, Applicant has amended claim 19 to recite "storing the list in a memory of a monitoring computer system." As discussed above with respect to claim 16, Liu does not teach or suggest discovery of nameservers, nor does Liu teach a monitoring computer that stores a list of discovered nameservers. Further, claim 19 was amended to recite "storing the list of nameservers in a memory of a monitoring computer system, the list of nameservers to be queried by the monitoring computer system to determine namespace mapping violations; determining a first mapping in a domain naming system, the act of determining the first mapping comprising an act of obtaining an authoritative mapping from an authoritative source; determining a second mapping in the domain naming system, the act of determining a second mapping comprising acts of querying a nameserver of the list of nameservers to be queried and receiving a response from the nameserver, the response containing the second mapping, wherein the first mapping is a first namespace mapping that maps a first name to a first resource and the second mapping is a second namespace mapping that maps a second name to a second resource; comparing the first mapping to the second mapping and identifying at least one discrepancy between the first and second mapping; and generating and sending an alert message to a user, the alert message indicating the at least one discrepancy between the first and second mapping." Liu does not disclose determining namespace mapping violations, and maintaining lists of nameservers to be queried by a monitoring computer system. For at least these reasons, Liu does not anticipate claim 19 as amended. Claim 20 depends from claim 19 and is allowable for at least the same reasons.

Accordingly, withdrawal of these rejections is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50/2762.

Respectfully submitted,
Gerald R. Malan, Applicant

By: /Edward J. Russavage/
Edward J. Russavage, Reg. No. 43,069
LOWRIE, LANDO & ANASTASI, LLP
One Main Street
Cambridge, Massachusetts 02142
United States of America
Telephone: 617-395-7000
Facsimile: 617-395-7070

Docket No.: A0781-701810
Date: November 24, 2008